



741A  
5-14-02  
M.L.

Atty. Dkt. No. 068398-0104

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Applicant: Virgil D. Gligor et al.

Title: AUTHENTICATION METHOD AND SCHEMES FOR DATA  
INTEGRITY PROTECTION

Appl. No.: 09/818,608

Filing Date: March 28, 2001

Examiner: Unassigned

Art Unit: 2131

RECEIVED  
SEP 27 2001  
Technology Center 2100

PRELIMINARY AMENDMENT

Commissioner for Patents  
Washington, D.C. 20231

Sir:

Prior to examination of the application, applicants respectfully request that the  
above-identified prior application be amended as follows:

In the Specification:

Please amend the specification as follows:

Page 15, paragraph 56:

In a further aspect, the present invention comprises the steps of: generating said  
counter anew for every new key; initializing generated counter to a constant value; for  
each message being signed using key, incrementing said counter by one; and outputting  
said counter as an output block of the authentication scheme.

Page 16, paragraph 61:

In a further aspect, the present invention comprises the steps of: creating a  
secret random vector block of  $\ell$  bits in length; performing the same randomization  
function as that used at a signing method for determining an authentication tag over the  
plurality of plaintext blocks and the secret random vector block to create a plurality of  
input blocks each of  $\ell$  bits in length; wherein performing the randomization function